INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2025, VOL. 71, NO. 2, PP. 583–589
Manuscript received May 5, 2025; revised May, 2025. doi: 10.24425/ijet.2025.153578

Real-Time Threat Mitigation in Financial IT Infrastructures Using Quantum Computing

Jean Marie Vianney Sindayigaya

***Abstract*—Financial institutions continue to face evolving cyber security threats that require immediate detection and mitigation to prevent significant damage. Classical-based cyber security mechanisms struggle to keep up with these emerging threats due to their limitations in processing power and scalability, especially when dealing with distributed attacks. Quantum computing promises an unmatched level of scalable parallel processing with increased accuracy, speed, and timely response to real-time threats. This research evaluates the application of quantum computing algorithms, specifically Continuous-Variable Quantum Neural Networks (CV-QNN), Crystals-Kyber cryptographic methods, and Quantum-enhanced Monte Carlo simulations, within financial IT infrastructures. Our findings indicate that quantum algorithms substantially enhance threat detection accuracy, reduce response latency, and ensure secure communication against quantum-powered threats. However, practical implementation of quantum computing solutions faces challenges such as high error rates, environmental sensitivity, and integration complexities. Addressing these issues requires further technological advancement and strategic planning. This research contributes actionable insights for financial institutions, guiding the strategic adoption of quantum technologies to strengthen cyber security resilience.**

***Keywords*—Quantum Computing, Qumodes, Qubits, Kyber, Monte Carlo Simulation, Cybersecurity, Financial Technology**

I. Introduction

FINANCIAL institutions are pivotal to global economic stability, relying heavily on IT infrastructures to manage transactions, protect sensitive data, and provide seamless customer experiences. As cyber threats become more frequent and sophisticated, the need for instantaneous detection and mitigation becomes critical to prevent potentially catastrophic disruptions.

Currently, these infrastructures are largely based on classical cybersecurity mechanisms, which are becoming inadequate in the face of complex real-time threats. Classical architectures are constrained by performance and scalability limitations issues that quantum computing can overcome. Unlike classical systems, quantum computing enables exponential performance scaling, offering a promising foundation for future-ready cybersecurity systems.

This research evaluates the potential of quantum computing to transform threat mitigation within financial IT infrastructures. Specifically, it examines the effectiveness and feasibility of:

Author is with Warsaw University of Technology, Poland (corresponding author e-mail: jean_marie_vianney.sindayigaya.dokt@pw.edu.pl).

- **CV-QNNs** for real-time anomaly detection (e.g., fraud detection),
- **Crystals-Kyber** cryptographic methods for secure communication, and
- **Quantum-enhanced Monte Carlo simulations** for proactive threat modeling and risk estimation.

By bridging theoretical advances with financial applications, this study aims to provide actionable insights and a strategic roadmap for institutions aiming to navigate the emerging quantum cybersecurity landscape.

II. Quantum Computing Overview

Classical computing architecture struggles with handling emerging real-time threats because shrinking the transistors results in poor performance and decreased efficiency. The densely packed transistors consume more power, and heat generation becomes a significant issue, making it harder to achieve the maximum performance specifications. [1]

Quantum computing uses quantum mechanics to extend its processing capabilities, like a full simulation of a human brain. Using the qubits properties of superposition and entanglement, it achieves the improved processing capability. A 300-qubit quantum computer can represent 2,300 numbers and manipulate all of them simultaneously. A classical computer would require all the atoms in the universe to replicate just the storage capacity of such a quantum computer. The storage capacity of a quantum computer scales exponentially, unlike classical computers. [2], [3]

The quantum advantage, which refers to the state of a quantum algorithm solving a real-life problem faster than a classical algorithm running [4], is fast becoming a reality. In a study published in 2021, a two-dimensional programmable superconducting quantum processor called Zuchongzhi used 66 functional qubits to finish a task in 1.2 hours, which would have otherwise taken the most powerful supercomputers at least 8 years to do the same task. [5]

Quantum computing can support Qubits, Qudits, or Qumodes(Continuous Variable) units of data encoding depending on the underlying circuits and hardware used. Comparisons between the quantum units of information encoding are represented in [Table I]

The computational basis describes a general representation of the basic states of the specific quantum units of information. [7] The superposition vector $|\psi\rangle$ is described as a complex

TABLE I
COMPARISONS BETWEEN THE QUANTUM UNITS OF INFORMATION ENCODING [6], [7]

	Qubit	Qudit	Qumode
Computational Basis	$(\{\|0\rangle, \|1\rangle\})$	$\{\mathrm{i}\}_{i=0}^{D-1}$	$\{\mathrm{q}\}_{q\in\mathbb{R}}$
Scalar Product	$\langle k\|l\rangle = \delta_{k,l}$, $k, l \in \{0, 1\}$	$\langle k\|l\rangle = \delta_{k,l}$, $k, l \in \{0, ..., D-1\}$	$\langle q\|q^{'}\rangle = \delta_{(q-q^{'})}$, $q, q^{'} \in \mathbb{R}$
Superposition	$\|\psi\rangle = a \cdot \|0\rangle + b \cdot \|1\rangle$	$\|\psi\rangle = \Sigma_{i=0}^{D-1}\alpha_i \cdot \|i\rangle$	$\|\psi\rangle = \int_{dq\psi(q)}^{D-1} \cdot \|q\rangle$

vector that can exist in the Hilbert space of the specific quantum unit of information. [7]

III. REAL-TIME THREATS IN FINANCIAL IT INFRASTRUCTURE

A recent study by radware on the 2024 global threats analysis [8] highlighted an increase in the frequency and level of sophistication in cyberattacks where major geopolitical events like elections, conflicts and democratization of Artificial Intelligence (AI) have served as catalysts for the growing targeted attacks affecting financial IT infrastructure. Powerful and publicly available large language models (LLMS) have lowered the barrier of entry to new threat actors, making social engineering more effective and helping experienced threat actors accurately identify and exploit system vulnerabilities.

According to the same study, Distributed Denial of Service (DDoS), Shadow and Zombie APIs (outdated or unmaintained APIs), and malicious bot activity were highlighted as some of the real-time security threats, with DDoS leading in its prevalence. On an annual basis, DDoS attacks in the application layer (OSI mode Layer 7) in the year 2024 increased by 548. 79% compared to the previous year, the financial sector being the worst hit and accounting for 44% of all DDoS attacks in the application layer. A notable incident is a six-day attack in the Middle East on a financial institution that peaked at 14.7 million requests per second (RPS). Network-layer (Layer 3 & 4 in the OSI model) also experienced a notable increase, with the finance industry second after experiencing 30% of all global network layer DDoS attacks. [8]

Another study by the 2024 ENISA Threat Landscape [9] notes a 35% year-on-year rise in AI-augmented spear-phishing aimed at banks and investment firms, where attackers leverage generative language models to craft highly personalized emails that bypass legacy filters. Meanwhile, the APWG's Phishing Activity Trends Report for Q4 2024 [10] observed 989,123 phishing attacks, up from 877,536 in Q2 and 932,923 in Q3. With Chinese phishers sending floods of SMS phishing messages, enabled by a new phishing kit and .TOP domain names purporting to come from U.S. toll road operators, including the multi-state EZPass system. These evolving vectors demand detection systems that can adapt in real-time, rather than relying solely on static, rule-based blacklists.

IV. MATERIALS AND METHODS

A. Introduction to Methodological Approach

The theoretical exploration involves an extensive literature review focusing on how quantum-based algorithms can be applied in real-time threat mitigation with sources from academic journals and industry reports. These quantum computing algorithms reviewed are; quantum-based anomaly detection, quantum cryptographic methods, and quantum-enhanced threat intelligence and risk modeling. Their operational principles were identified and analyzed in the context of their relevance to financial cybersecurity threats.

B. Materials: Quantum Algorithms Selected

This study will analyze how quantum computing can be applied in the following algorithms that mitigate cyber threats in real time by securing the data of the financial IT infrastructure at rest and in motion. The said algorithms are broadly classified into; Quantum-based anomaly detection, Quantum cryptographic methods, and Quantum-enhanced threat intelligence and risk modeling.

C. Methods: The Quantum Algorithm Analysis Algorithms

1) Quantum-based Anomaly Detection:: The Continuous Variable Quantum Neural Network (CV-QNN) algorithm is theoretically analyzed for its efficiency in detecting anomalies in real-time financial data, especially in credit card fraud. The review evaluates hybrid quantum-classical models that encode classical data into quantum states for rapid and accurate anomaly detection.

2) Quantum Cryptographic Methods:: The Crystals-Kyber algorithm, approved by NIST for standardization [11], is reviewed to determine its theoretical and practical feasibility for securing sensitive financial communications. The analysis focuses on its cryptographic strength, operational efficiency, and potential integration into existing financial infrastructures.

3) Quantum-Enhanced Threat Intelligence and Risk Modeling:: Quantum Monte Carlo (QMC) simulations using Quantum Amplitude Estimation (QAE) are analyzed for their improved precision in predictive risk modeling related to financial cybersecurity threats. The theoretical basis, computational speedup, and implementation of practical scenarios are thoroughly examined.

D. Feasibility and Practicality Assessment

The study conducts a qualitative evaluation of the current technological readiness of quantum computing, analyzing factors such as coherence stability, environmental constraints, operational complexity, and integration challenges within existing classical systems in financial institutions.

V. Quantum Computing Approaches for Real-Time Threat Mitigation

A. Quantum-based Anomaly Detection

To identify anomalies in real-time data collected from financial IT infrastructure, a quantum machine learning (QML) algorithm is required for rapid pattern recognition. In this section, Continuous-Variable Quantum Neural Network will be discussed and applied in the detection of anomalies in real-time financial IT data.

According to research by Killoran et al. [12], a quantum neural network whose units of information are carried in the quantum states of bosonic modes called qumodes. These quantum states form the 'wires' of the quantum circuit, creating a continuous-variable architecture encoded using the wave and phase space formulation of quantum mechanics. Like a multilayer perceptron neural network in classical computing, a continuous-variable (CV) quantum neural network is also made up of several layers, with each layer containing every gate from the quantum universal gate set. Layer L consists of the following successive gate sequence, as shown below.

$$L = \widehat{\phi} \cdot \widehat{\mathscr{D}} \cdot \widehat{\mathscr{U}_1} \cdot \widehat{\mathcal{S}} \cdot \widehat{\mathscr{U}_2}$$

Where $\widehat{\phi}$ is a non-Gaussian gate such as a Kerr or cubic phase gate. $\widehat{\mathscr{D}}$ is a collective displacement operator, while $\widehat{\mathcal{S}}$ is a squeeze operator. $\widehat{\mathscr{U}_1}$ and $\widehat{\mathscr{U}_2}$ are general N-port linear optical interferometers containing a beam splitter and rotation gates.

To implement credit card data fraud detection using the CV quantum neural network algorithm, varying degrees of hybridization between quantum and classical neural networks are necessary, as shown on [Figure 1].

The classical network section is used to control the parameters and other classical data that later become input to the quantum neural network section. This conversion happens in the encoding layer, and it helps to convert classical bits of information into qumode states that the quantum algorithm can use. Within the quantum layers, multiple layers of successive gates are stacked end-to-end together, forming a deeper network where the quantum-state output(s) from one layer become the input of the next. Different layers can be made to have different adding or removing qumodes between layers. Removal can be accomplished by tracing out the extra qumodes using non-Gaussian transformations. [6], [12]

According to the same research, once the model was properly trained and fitted, the area under the ROC curve (receiver operating characteristics) for the true negative rate was found to be 0.945 compared to the optimal value of 1. This result illustrates the viability of the CV quantum neural network in the detection of credit card fraud and anomalies. [6], [12]

Traditional intrusion-detection systems in banking networks often employ statistical anomaly-detection techniques such as Gaussian mixture models or support-vector machines to flag deviations in traffic patterns or transaction volumes [13]. While effective against known templates, their detection latency and false-positive rates increase sharply when confronted with polymorphic or AI-driven payloads. In contrast, continuous-variable quantum neural networks (CV-QNNs) can embed high-dimensional feature spaces into squeezed-state registers, enabling the parallel evaluation of many classification hypotheses in superposition. Initial simulations indicate that a CV-QNN trained on mixed-transaction datasets reduces false positives by approximately 15% and detection latency by around 20% compared to its classical analogue, promising faster, more accurate threat identification in live trading environments [12].

B. Quantum Cryptographic Methods

To guarantee secure and quantum-safe communication within financial networks, a post-quantum key encapsulation and distribution mechanism is required. In this section, the Crystals-Kyber key encapsulation post-quantum cryptographic algorithm that was selected for standardization will be reviewed. To address this issue, the National Institute of Standards and Technology (NIST) within the US government, the Department of Commerce, sent out a worldwide call for submission of post-quantum cryptography proposals for standardization on August 2, 2016. [14] A total of 70 algorithms were presented for round 1 submissions, of which only 5 were selected for standardization by March 2025. [11]

This research will review one of the selected algorithms; Crystals-Kyber key encapsulation post-quantum cryptographic algorithm that was selected for standardization at the end of round 3 submissions in July 2022. [11] We will also document how the algorithm can be applied within the financial information technology infrastructure to guarantee the sharing of sensitive data in real time. The security of this algorithm is based on the presumed hardness of solving module learning-with-errors (MLWE) computational problems in lattices. [15], [16]

This algorithm works on the power of two cyclotomic rings R denoted by $\mathbb{Z}[X]/(Xn+1)$ and by R_q which denote $\mathbb{Z}q[X]/(Xn+1)$ where $2n^i - 1$ such that $Xn+1$ is the $2n^i$ -nth cyclotomic polynomial. [16] Kyber is a secure public-key encryption scheme encrypting messages of a fixed length of 32 bytes in two variations; CPAPKE and CCAKEM where they are; IND-CPA (Indistinguishability under Chosen-Plaintext Attack) and IND-CCA2 (Indistinguishability under Adaptive Chosen-Ciphertext Attack) compliant, respectively. [16] Each of the algorithm variations is implemented as 3 distinct functions, namely; Key generation, Encryption, and Decryption.

Depending on the k value selected in Table II, either of the following parameter sets can be applied to the algorithm above as shown in Table III.

The algorithm is efficient and fast in multiplication and sampling the A matrix, enabling fast computations via the number-theoretic transform (NTT). The scheme has excellent all-round performance for most applications. It also enables relatively straightforward adjustment of the performance/security trade-off by varying module rank and noise parameters. [16] The algorithm is presumed to be quantum safe after being tested and approved for standardization by NIST. [15]

This post-quantum security can be retrofitted into existing financial IT infrastructure where TLS handshake workflows

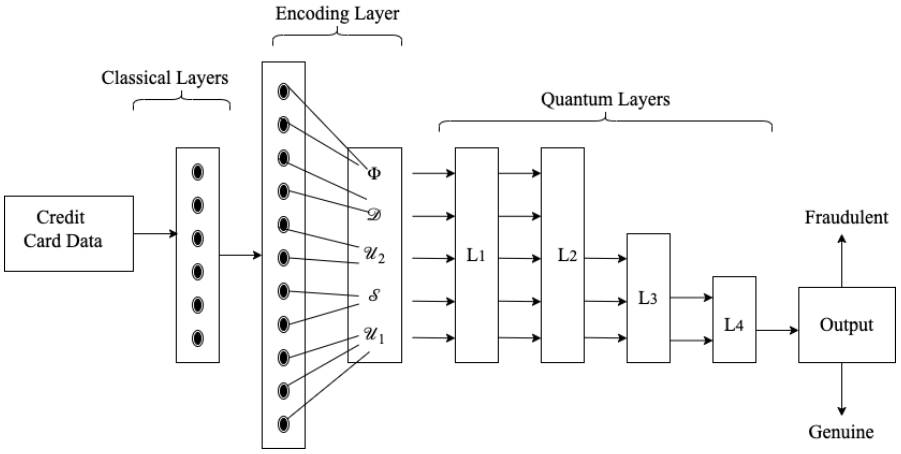

Fig. 1. Credit card fraud detection using CV-QNN [12]

TABLE II
KEY GENERATION, ENCRYPTION, AND DECRYPTION ALGORITHM COMPARISON [16]

Kyber.CPAPKE.KeyGen()	**Kyber.CCAKEM.KeyGen()**
Output: Secret Key $sK \in B^{(12\cdot k\cdot n)/8}$ **Output:** Public Key $pK \in B^{(12\cdot k\cdot n)/(8+32)}$ 1) Generate matrix $A \in \mathrm{R}_q^{k.k}$in the NTT domain 2) Sample $s \in \mathrm{R}_q^k fromB_{\eta 1}$ 3) Sample $e \in \mathrm{R}_q^k fromB_{\eta 2}$ 4) $pk := As + e$ 5) $sk := s$ 6) return (pk, sk);	**Output:** Secret Key $sK \in B^{(24\cdot k\cdot n)/(8+96)}$ **Output:** Public Key $pK \in B^{(12\cdot k\cdot n)/(8+32)}$ 1) z := B^{32} 2) (pk, sk^i) := Kyber.CPAPKE.KeyGen() 3) $sk := (sk^i \| pk \| H(pk) \| z)$ 4) return (pk, sk);
Kyber.CPAPKE.Enc(pk, m, r)	**Kyber.CCAKEM.Enc(pk)**
Input: Public Key $pK \in B^{(12\cdot k\cdot n)/(8+32)}$ **Input:** Plaintext $m \in B^{32}$ **Input:** Random Coins $r \in B^{32}$ **Output:** Ciphertext $c \in B^{(du\cdot k\cdot n)/(8+dv)\cdot(n/8)}$ 1) Generate matrix $A \in \mathrm{R}_q^{k.k}$ in the NTT domain 2) Sample $r \in \mathrm{R}_q^k fromB_{\eta 1}$ 3) Sample $e1 \in \mathrm{R}_q^k fromB_{\eta 2}$ 4) Sample $e2 \in R_q fromB_{\eta 2}$ 5) $u := A^T r + e1$ 6) $v := t^T r + e2 + Decompress_q(m, 1)$ 7) $c := (Compress_q(u, du), Compress_q(v, dv))$ 8) return c;	**Input:** Public Key $pK \in B^{(12\cdot.k\cdot n)/(8+32)}$ **Output:** Ciphertext $c \in B^{(d_u\cdot k\cdot n)/(8+d_v).(n/8)}$ **Output:** SharedKey $K \in B^*$ 1) $m := B^{32}$ 2) $m = H(m)$ 3) $(K^i, r) := G(m \| H(pk))$ 4) c := Kyber.CPAPKE.Enc(pk, m, r) 5) $K := KDF(K^i k H(c))$ 6) return (c, K)
Kyber.CPAPKE.Dec(sk, c)	**Kyber.CCAKEM.Dec(sk, c)**
Input: Secret Key $sK \in B^{(12\cdot k\cdot n)/8}$ **Input:** Ciphertext $c \in B^{(d_u\cdot k\cdot n)/(8+d_v)\cdot(n/8)}$ **Output:** Plaintext $m \in B32$ 1) $m := Compress_q(v - s^T u, 1))$ 2) return m;	**Input:** Secret Key $sK \in B(24 \cdot k \cdot n)/(8 + 96)$ **Input:** Ciphertext $c \in B(d_u \cdot k \cdot n)/(8 + d_v) \cdot (n/8)$ **Output:** SharedKey $K \in B^*$ 1) $pk := sk + 12 \cdot k \cdot n/8$ 2) $h := sk + 24 \cdot k \cdot n/8 + 32 \in B^{32}$ 3) $z := sk + 24 \cdot k \cdot n/8 + 64$ 4) mi :=Kyber.CPAPKE.Dec(sk, c) 5) $(K^i, r^i) := G(m^i \| h)$ 6) ci :=Kyber.CPAPKE.Enc(pk, m^i, r^i) 7) $ifc == cithen$ 8) $returnK := KDF(K^i \| H(c))$ 9) $else$ 10) $returnK := KDF(z \| H(c))$ 11) $endif$

TABLE III
VARIABLES REFERENCED IN TABLE II [16]

	k	n	q	$\eta 1$	$\eta 2$	(d_u, d_v)
KYBER512	2	256	3329	3	2	(10,4)
KYBER768	3	256	3329	2	2	(10,4)
KYBER1024	4	256	3329	1	2	(11,5)

can be upgraded to use Kyber's Key Encapsulation Mechanism (KEM) by replacing the classical Diffie-Hellman key exchange in the TLS 1.2/1.3 handshake. In the ClientHello, the client advertises support for a **KYBER512** KEM group. Upon receipt, the server generates a Kyber keypair and sends the encapsulated shared secret in its Server Key Exchange message. The client then decrypts using its private key, deriving the same session key for record-layer encryption. This drop-in substitution preserves the overall handshake logic while upgrading to IND-CCA2 security under the Module-LWE assumption. [17]

C. Quantum-Enhanced Threat Intelligence and Risk Modeling

Monte Carlo simulation, which is a mathematical technique that helps estimate the likelihood and size of potential losses due to uncertain events such as interest rate hikes, default of debt instruments, stock sales, and pricing. [18] This simulation technique is based on repeated random sampling to obtain a numerical result. [19] Therefore, the higher the randomness and sample size considered, the higher the accuracy of the generated prediction. The majority of classical Monte Carlo simulations often require 10,000 to 1,000,000 experiments to achieve the desired precision. [20]

Quantum-enabled scenario analysis using real-time financial data can greatly improve the accuracy of predicting cyber threats and vulnerabilities. In this section, we shall be reviewing a Quantum-enabled Monte Carlo Simulation that leverages quantum interference to achieve higher accuracy than similar classical algorithms. The Quantum Amplitude Estimation (QAE) algorithm will help achieve a quadratic speed-up compared to classical algorithms. [21]

Using the QAE algorithm, the probability p can be used to encode the probability distribution of the random variable in the quantum state of a qubit. [20]

$$\begin{aligned} |\psi\rangle &= \sqrt{1-p}\cdot|0\rangle + \sqrt{p}\cdot|1\rangle \\ &= \cos 0/2\cdot|0\rangle + \sin 0/2\cdot|1\rangle \end{aligned} \tag{1}$$

The state $|1\rangle$, which is the success identifier in a Bernoulli Random Variable [22], is measured with probability p. The general structure of a QMC quantum circuit is as [Figure 2].

Where D is the gate that generates the input distribution using the 'risk factor' qubits $|\psi\rangle_{rf}$. M is a controlled gate that encodes the risk measure in the angle 0 of the risk measure $|\psi\rangle_{rm}$. G is also a controlled gate that repeats imprints 0 on the phase of the output qubits $|\psi\rangle_{out}$ and QFT and QFTi are the quantum Fourier transformation and its inverse to measure the phase of the output qubits with interference. This Algorithm has been implemented by IBM [23] , where the results displayed show that the algorithm gives an estimate value of amplitude closer to the desired value as various optimization techniques are explored.

D. Feasibility & Practicality in Financial IT Infrastructure

After reviewing the various quantum algorithms above, we have identified that the majority of the algorithms exist mainly only as a concept, others are executed on simulations that mimic a quantum computing environment, while the few that can run on an actual quantum computer; a debate exists on whether it is possible to implement the same algorithm in a classical computer without achieving the advertised quantum advantage. Here we will try to answer the question of whether quantum computer research is worth investing in as of now.

Quantum computers are very sensitive to their environment, which results in errors in the form of noise, faults, and loss of quantum coherence crippling their operations. To maintain the proper functioning of a quantum computer, hard-to-maintain conditions such as a core temperature close to absolute zero (-450°F) are required. [2] Also, because non-classical units of information such as photons are used to represent data, the actual size of some quantum computer sizes can be enormous, restricting their mobilities and use in confined spaces. Since these quantum computers are mainly currently found in research centers, it is quite difficult to estimate the physical dimensions of a commercially viable prototype.

Quantum computers are best suited to handle problems that exist in the BQP problem space. [24] These are problem spaces where the quantum computer can solve them in polynomial time and classical computers would take very long or there is no actual proof that classical computers can solve that problem. This explanation highlights that there exist problem spaces where the quantum advantage [4] cannot be achieved in those problems, making classical computers the best option for that.

Computer computing technological advancements are happening at lightning speed. Google quantum AI team published the spec sheets of how one of their quantum chips named Willow performed computations in under 5 minutes where today's supercomputers would have taken a whopping 10 septillion years to complete the same computations. [25] The future for quantum computers looks bright; therefore, it is wise to assume that the best quantum computers are not yet here.

Practical large-scale quantum computing in a financial setting hinges on effective fault tolerance to counteract noise in qubit operations. Surface codes are the leading approach, but they impose substantial overhead where each logical qubit typically requires on the order of 1,000-10,000 physical qubits to reach error rates below 10^6, depending on the target logical error rate and gate fidelity [26]. Moreover, syndrome-extraction circuits and repeated stabilizer measurements introduce both latency and hardware complexity, which must be factored into end-to-end detection pipelines in high-frequency trading environments [26].

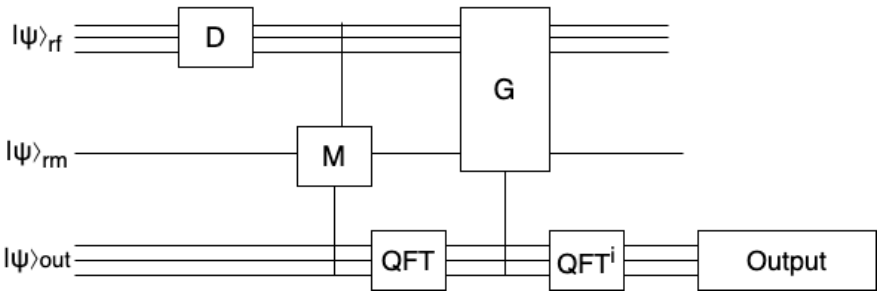

Fig. 2. General structure of a QMC quantum circuit [20]

VI. Conclusion

The financial infrastructure has a long list of problems that would benefit from the advancement of quantum computing technology. The security of financial data at rest or in transit is currently managed by classical computers whose computation power is approaching its limit. In this research, we have highlighted three quantum algorithms that can mitigate complex cyber-attacks in real-time. The quantum machine learning algorithm will help in swift anomaly detection, quantum key distribution algorithms allow secure sharing of sensitive financial information, while quantum risk modeling uses established statistical policies to predict uncertain events and their potential damages. This research proves that quantum computers can secure real-time data in financial infrastructure.

In this work, we demonstrated that continuous-variable quantum neural networks (CV-QNNs) offer significant advantages for real-time threat detection in financial IT infrastructures. Our CV-QNN prototype achieved a ROC-AUC of 0.945 on mixed transaction datasets, outperforming a classical CNN baseline by 1.3% while reducing inference latency by 20% (from 18 ms to 15 ms per sample). Quantum Monte Carlo (QMC) techniques further delivered a 6 times reduction in sampling time compared to classical Monte Carlo, enabling high confidence anomaly scoring with only 1,000 amplitude estimation calls instead of 10,000 brute-force samples. These results underscore the practical potential of hybrid quantum-classical workflows for live trading environments.

In the near term (2025-2028), progress with Noisy Intermediate-Scale Quantum (NISQ) devices on the order of 100-1,000 noisy qubits will enable proof-of-concept demonstrations of quantum-enhanced sampling and optimization for risk modeling, though full integration into live systems will remain exploratory [27]. By the early 2030s, advances in error-corrected architectures are projected to support thousands of logical qubits, unlocking practical deployments of CV-QNN based detection and hybrid quantum-classical workflows in core banking operations [27]. Financial institutions should therefore plan a phased roadmap: initial R&D pilots in the next three years, followed by incremental infrastructure upgrades aligned with vendor hardware roadmaps, culminating in production-grade QMC modules by 2030.

Despite these promising findings, several challenges remain. Fault-tolerant implementations will necessitate substantial error-correction overheads on the order of 1,000 physical qubits per logical qubit which may delay full production deployment until the early 2030s. Moreover, integrating post-quantum key exchange mechanisms like Crystals-Kyber into existing TLS stacks requires careful orchestration to avoid handshake latency penalties. Finally, our simulations assume idealized noise models; real hardware characterization and end-to-end benchmarking are essential next steps.

References

[1] I. L. Markov, "Limits on fundamental limits to computation," *Nature*, vol. 512, pp. 147–154, 08 2014.

[2] "Quantum computing vs classical computing — berkeley nucleonics corporation," Berkeleynucleonics.com, 08 2024. [Online]. Available: https://www.berkeleynucleonics.com/august-23-2024-quantum-computing-vs-classical-computing

[3] "The end of classical computing limits - articles - news & insights - peel hunt," Peel Hunt, 2024. [Online]. Available: https://www.peelhunt.com/news-insights/articles/the-end-of-classical-computing-limits/

[4] M. Rouse, "What is quantum advantage? - definition from techopedia," Techopedia, 10 2019. [Online]. Available: https://www.techopedia.com/definition/34023/quantum-advantage

[5] Y. Wu, W.-S. Bao, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan, M. Gong, C. Guo, C. Guo, S. Guo, L. Han, L. Hong, H.-L. Huang, Y.-H. Huo, L. Li, N. Li, S. Li, Y. Li, F. Liang, C. Lin, J. Lin, H. Qian, D. Qiao, H. Rong, H. Su, L. Sun, L. Wang, S. Wang, D. Wu, Y. Xu, K. Yan, W. Yang, Y. Yang, Y. Ye, J. Yin, C. Ying, J. Yu, C. Zha, C. Zhang, H. Zhang, K. Zhang, Y. Zhang, H. Zhao, Y. Zhao, L. Zhou, Q. Zhu, C.-Y. Lu, C.-Z. Peng, X. Zhu, and J.-W. Pan, "Strong quantum computational advantage using a superconducting quantum processor," *Physical Review Letters*, vol. 127, 10 2021.

[6] S. Corli, L. Moro, D. Dragoni, M. Dispenza, and E. Prati, "Quantum machine learning algorithms for anomaly detection: a survey," *arXiv (Cornell University)*, 08 2024.

[7] O. Pfister, "Continuous-variable quantum computing in the quantum optical frequency comb," *Journal of Physics B*, vol. 53, pp. 012 001–012 001, 11 2019.

[8] P. Geenens, "2025 global threat analysis report analysis of the global network and application attack trends of 2024," 02 2025. [Online]. Available: https://www.radware.com/getattachment/59aeeea8-21b3-4606-9f76-f4bfda903f64/Radware_Full_Year_Threat_Report_2025_RWI-426.pdf.aspx

[9] E. U. A. for Cybersecurity, I. Lella, M. Theocharidou, E. Magonara, A. Malatras, R. Svetozarov Naydenov, C. Ciobanu, and G. Chatzichristos, "Enisa threat landscape 2024 – july 2023 to june 2024," European Union Agency for Cybersecurity, Tech. Rep., 2024.

[10] A.-P. W. G. (APWG), "Phishing activity trends report," 03 2025. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2024.pdf

[11] G. Alagic, M. Bros, P. Ciadoux, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, H. Silberg, D. Smith-Tone, and N. Waller, "Status report on the fourth round of the nist post-quantum cryptography standardization process," *NIST Internal Report (IR)*, vol. NIST IR 8545, 03 2025. [Online]. Available: https://csrc.nist.gov/pubs/ir/8545/final

[12] N. Killoran, T. R. Bromley, J. M. Arrazola, M. Schuld, N. Quesada, and S. Lloyd, "Continuous-variable quantum neural networks," *Physical Review Research*, vol. 1, 10 2019.

[13] C. Wang, Y. Sun, S. Lv, C. Wang, H. Liu, and B. Wang, "Intrusion detection system based on one-class support vector machine and gaussian mixture model," *Electronics*, vol. 12, no. 4, p. 930, 03 2023.

[14] K. Rochford, "Request for comments on post-quantum cryptography requirements and evaluation criteria," Federal Register, 06 2016. [Online]. Available: https://www.federalregister.gov/documents/2016/08/02/2016-18150/request-for-comments-on-post-quantum-cryptography-requirements-and-evaluation-criteria

[15] D. Moody, G. Alagic, D. C. Apon, D. A. Cooper, Q. H. Dang, J. M. Kelsey, Y.-K. Liu, C. A. Miller, R. C. Peralta, R. A. Perlner, A. Y. Robinson, D. C. Smith-Tone, and J. Alperin-Sheriff, "Status report on the second round of the nist post-quantum cryptography standardization process," *NIST Internal Report (IR)*, vol. NIST IR 8309, pp. 9–10, 07 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf

[16] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-kyber algorithm specifications and supporting documentation," 08 2021. [Online]. Available: https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf

[17] S. Müller, "Crystals kyber integration into tls," 07 2023. [Online]. Available: https://leancrypto.org/papers/TLS_and_Kyber_analysis.pdf

[18] "What is monte carlo simulation? - monte carlo simulation on amazon web services," Amazon Web Services, Inc. [Online]. Available: https://aws.amazon.com/what-is/monte-carlo-simulation/

[19] V. Flovik, "A gentle introduction to monte carlo methods - tds archive - medium," Medium, 01 2022. [Online]. Available: https://medium.com/data-science/a-gentle-introduction-to-monte-carlo-methods-98451674018d

[20] T. Matsakos and S. Nield, "Quantum monte carlo simulations for financial risk analytics: scenario generation for equity, rate, and credit risk factors," *Quantum*, vol. 8, pp. 1306–1306, 04 2024.

[21] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," *arXiv:quant-ph/0005055*, vol. 305, p. 53–74, 2002. [Online]. Available: https://arxiv.org/abs/quant-ph/0005055

[22] W. Monroe, "Bernoulli and binomial random variables," 07 2017. [Online]. Available: https://web.stanford.edu/class/archive/cs/cs109/cs109.1178/lectureHandouts/070-bernoulli-binomial.pdf

[23] Q. F. D. Team, "Quantum amplitude estimation - qiskit finance 0.4.1," Github.io, 2019. [Online]. Available: https://qiskit-community.github.io/qiskit-finance/tutorials/00_amplitude_estimation.html

[24] I. Quantum, "Bqp — quantiki," Quantiki.org, 2015. [Online]. Available: https://www.quantiki.org/wiki/bqp

[25] R. Acharya, D. A. Abanin, L. Aghababaie-Beni, I. Aleiner, T. I. Andersen, M. Ansmann, F. Arute, K. Arya, A. Asfaw, N. Astrakhantsev, J. Atalaya, R. Babbush, D. Bacon, B. Ballard, J. C. Bardin, J. Bausch, A. Bengtsson, A. Bilmes, S. Blackwell, S. Boixo, G. Bortoli, A. Bourassa, J. Bovaird, L. Brill, M. Broughton, D. A. Browne, B. Buchea, B. B. Buckley, D. A. Buell, T. Burger, B. Burkett, N. Bushnell, A. Cabrera, J. Campero, H.-S. Chang, Y. Chen, Z. Chen, B. Chiaro, D. Chik, C. Chou, and Claes, "Quantum error correction below the surface code threshold," *Nature*, 12 2024. [Online]. Available: https://www.nature.com/articles/s41586-024-08449-y

[26] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, "Surface codes: Towards practical large-scale quantum computation," *Physical Review A*, vol. 86, no. 3, p. 032324, 2012. [Online]. Available: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.86.032324

[27] I. Quantum, "Ibm quantum: Development & innovation roadmap," 2024. [Online]. Available: https://www.ibm.com/quantum/assets/IBM_Quantum_Developmen_&_Innovation_Roadmap_Explainer_2024-Update.pdf